computers being provided with browser programming for accessing and/or displaying files and other data between the sender and receiver computers over the Internet;

establishing at least one additional transmission of data between the sender computer Web site and the receiver computer gateway;

adaptively determining the number of additional transmissions between the sender computer Web site and the receiver computer gateway site;

transmitting the data during at least one of the additional transmissions; and

authenticating each transmission in which data is transmitted. - -

REMARKS

Reconsideration of this Application is respectfully requested. Claims 1-15 are amended, without prejudice or disclaimer. New claims, i.e., independent claims 16 and 17, are added. Claims 1-17 are now in this case.

Initially, the Examiner noted that the captioned Application lacks formal drawings, but that the informal drawings filed in the Application are acceptable for examination purposes. The Examiner commented that when the Application is allowed, Applicants will be required to submit new formal drawings.

The Examiner then rejected claims 1-15 under 35 U.S.C. § 112, second paragraph, for indefiniteness. According to the Examiner, the phrase "authenticating transferred data between a sender and receiver" in claim 1 is vague and indefinite. The Examiner also indicates that this claim and the dependent claims that follow do not indicate details of the invention. She explained that the claims are written too broadly to accurately determine

limitations of the invention.

As an Examiner's note, she also indicated that while on page 8 of the Specification, Applicants indicate "a server 14 which are connected via a global network 16, such as the Internet", none of the claims identify "a server". In addition, the Examiner commented that although the phrase "the client computer 22 includes an Internet browser program 26" on page 8 of the Specification, none of the claims identify a "browser", "gateway" or "web page".

* * * * *

Next, the Examiner rejected claims 1-4 and 6-15 under 35 U.S.C. § 103(a) as being obvious and, therefore, unpatentable over Krishnamurthy et al., U.S. Patent No. 6,389,464, in view of Nickles, U.S. Patent No. 6,134,591. According to the Examiner, the limitation in claim 1 of "A method for authenticating transferred data between a sender and a receiver over an open network comprising the steps of- establishing a first secure transmission of data between the sender and the receiver" is taught by Krishnamurthy et al. (column 10, lines 48-65) as follows: "The home page 100 for the site server 12 is shown...managed devices and ports... The page preferably requires a system administration password 116". The limitation "establishing at least one additional transmission of data between the sender and the receiver" of claim 1, the Examiner asserts, is also set forth by Krishnamurthy et al. (column 16, lines 51-54) as "for a Get operation, the SNMP agent executes the call-back function". Regarding the element "adaptively determining the number of additional transmissions", the Examiner finds such to be disclosed also in Krishnamurthy et al. (column 12, lines 30-31) by the language "Reply length 166 is the total length of expected data in bytes". As for the

limitation "transmitting the data during at least one of the additional transmission; and", the Examiner takes the position that such is set forth by Krishnamurthy et al. (column 16, lines 43-47) as "With continued reference to FIG. 30, the input/output conversion tables 218 with the instrumentation drivers and the port configuration table 220 are used by the SNMP engine 84 to read the response from the device 14 and to write the requested value as the value of the instance of the MIB parameter".

The Examiner acknowledges that Krishnamurthy et al. do not teach the step of "authenticating each transmission in which data is transmitted". She then looks to Nickles which, she asserts, discloses such a limitation in column 11, lines 1-5, as: "Message 2 contains information that authorizes the object manager 104 of the application server 20 to perform specific tasks and provides the encryption keys and port addresses to be used for the transmission of data between the object and the gateway components of the web server 32".

The Examiner concludes that it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device management system of Krishnamurthy et al. to include a means to provide additional network security, as allegedly set forth by Nickles. One of ordinary skill in the art, she continues, would have been motivated to perform such a modification because with the increases in technology, an authentication method is needed to insure the identity of receiver and senders of communication. The Examiner cites, in this connection, column 2, lines 61 et seq. of Nickles which states "Thus, there is a need for a security system that enables a private network of computers to be accessible via an open network and that provides a higher level of security than that afforded by firewalls".

Regarding dependent claims 2 and 3, the Examiner determined that the limitations "wherein the number of additional transmissions is adaptively selected, at least in part, based upon the performance overhead of the system" and "wherein the number of additional transmissions is adaptively selected, at least in part, based upon monitored conditions" are disclosed by Krishnamurthy et al. Specifically, the Examiner cited the following language in column 17, lines 21-34: "The site server 12 of the present invention minimizes redundant commands to and responses from the device 14 by grouping related parameters to share a common response".

With reference to dependent claim 4, the Examiner takes the position that the element "wherein the number of additional transmissions is adaptively selected, at least in part, based upon a set of criteria that are used in an algorithm to determine the number of additional transmissions" is additionally described in Krishnamurthy et al. at column 8, lines 44-47, by the language "Dynamic loading allows the Web server 64 to start with a minimal amount of functionality". The phrase "the criteria selected from the group consisting of the frequency of transmissions between the sender and receiver", the Examiner continues, is disclosed in Krishnamurthy et al., column 12, lines 24-34, as "The time out value 164 indicates how long to wait for the response from the managed device". The claim element "the closeness of the sender to the source of the transactions, and" is purportedly taught in column 5, lines 56-59, as "The site server 12a can monitor activity of the SNMP-manageable devices and provide alternate paths". Last, the Examiner argues that the limitation "the usage patterns of the client" is described in Krishnamurthy et al., column 13, lines 19-23, by the language "some port types can be configured to match incoming patterns against known patterns to determine

whether the incoming string".

With respect to claim 6, the Examiner asserts that the claim element, "further comprising the step of transmitting at least one token to the receiver during the first secure transmission; wherein the data transmitting step further comprises transmitting at least one token along with the data; and wherein the authentication step comprises comparing, the at least one token transmitted during the additional transmission to the at least one token transmitted during the first secure transmission to determine whether the transmission is authentic", is taught by Nickles in column 7, lines 3-16, and more specifically, by the language "In the preferred operating environment, the computer system 16 first access a web server 32 when the computer system 16 desires to communicate...to the security server 24 indicating...then determines whether the computer 16 is authorized to access any of the application servers".

As for dependent claims 7 and 8, says the Examiner, "wherein the at least one token comprises a preselected number of tokens" and "herein the number of at least one transmissions corresponds to the preselected number of tokens" are further disclosed by Nickles, the Examiner citing the following language in column 7, lines 20-23: "Each device or workstation connected to a network is assigned a unique code. A standard network address is a 32-bit address field which is broken".

Referring now to dependent claim 9, the Examiner believes that the limitation "wherein the number of at least one transmissions is greater than the preselected number of tokens" is disclosed by Nickles at column 12, lines 5-7, namely, the language "In the system of the present invention, data sent by the object is blocked to reduce traffic".

As to dependent claim 10, the Examiner asserts that "wherein the number of at least

one transmissions is less than the preselected number of tokens" is set forth, in addition, by Nickles (column 11, lines 17-20) as "If the time-out value for the transaction is exceeded, the object execution for this transaction is aborted".

Next, the limitations "wherein the at least one additional transmission is conducted over an unsecure or open connection" and "wherein the at least one additional transmission is sent in plaintext" of claims 11 and 13, the Examiner continues, is shown in Krishnamurthy et al. at column 13, lines 33-40, by the language "whether a Trap message is to be sent to the SNMP manager 20 (as indicated on page 1956 in FIG. 22), or a facsimile or email message".

The phrase "wherein the first secure transmission is encrypted" of claim 12, according to the Examiner, is taught by Nickles in column 10, lines 21-23, specifically, by the language "The message 1 is encrypted".

Regarding dependent claim 14, the Examiner argues that the limitation "further comprising the steps of transmitting a checksum value during the first transmission and having the receiver verify that the checksum value is accurate by comparing the transmitted value to a checksum value generated using a similar checksum algorithm" is set forth in Nickles, column 10, lines 24-38, as "Digital signatures, or cryptographic checksums, are hashing techniques commonly known...A digital signature is caluculated [sic] as known by those skilled in art and compared to the digital signature in the decrypted message 1".

Last, with respect to dependent claim 15, the Examiner takes the position that the claim element "wherein the transmitted checksum value is based upon checksum values transmitted during previous transmissions" is taught by Nickles in column 10, lines 40-42, and, more specifically, by the language "The security server 24 accesses four transaction

tables to determine whether the user of computer system 16 is authorized to access the object".

* * * * *

Finally, the Examiner rejected claim 5 under 35 U.S.C. § 103(a) as obvious and, therefore, unpatentable over Krishnamurthy et al. in view of Nickles and further in view of Engel et al., U.S. Patent Application Publication No. 2003/0005144 A1, filed October 28, 1998. The Examiner admits that the combination of Krishnamurthy et al. and Nickles does not teach "wherein the algorithm is a statistical averaging algorithm". She then looks to Engel et al. which, she says, disclose, the same on page 5, in paragraph 0059, i.e., "The leaky bucket scheme uses 2 leaky buckets; one to monitor the peak rate and one to monitor the average rate".

The Examiner concludes that it would have been obvious to one having ordinary skill in the art at the time of the invention to modify the device management system over a secure network, allegedly taught by the combination of Krishnamurthy et al. and Nickles, to include a means adapt the number of transmission to a known average, as purportedly set forth by Engel et al. The Examiner explains that one of ordinary skill would have been motivated to perform such a modification because statistical information gained is practical in determining communication and limitations between devices. The Examiner specifically cites, in this connection, to Engel et al., page 3, paragraph 0025 et seq., namely, the language "An object of this invention is a system and method to reduce the delay, the delay variation...by rate shaping all other transmission that are destined to one of the two points".

* * * * *

Applicants wish to thank Examiner Tran for her kind assistance and helpful suggestions during the Interview on September 1, 2004. All of her suggestions are incorporated herein by the present Amendment.

First, claims 1 and 4 are amended to clarify that transfer of data occurs between a sender "computer" and a receiver "computer" of a "service broker system for interactive monitoring and control of data to and from Internet enabled devices of a sender/ receiver computer security system".

Claims 1 and 4 are also amended to better define the subject method of data transfer as one that is practiced over the Internet.

Additionally, Applicants have undertaken to amend claim 1 to more clearly delineate that the first secure transmission of data occurs between "a virtual gateway of the sender computer and a secure Web site of the receiver computer". In turn, claim 17 is added to cover the scenario where the first secure transmission of data occurs between "a Web site of the sender computer and a virtual gateway of the receiver computer".

Next, claim 1 is amended to illuminate the presence of "browser programming for accessing and/or displaying files and other data between the sender and receiver computers over the Internet".

Finally, dependent claims 2-15 are amended voluntarily to change "according to" to - - set forth in - - as a matter of desired style.

* * * * *

Accordingly, Applicants respectfully submit that claims 1 and 4 are amended to better define the invention without limiting effect. Withdrawal of the Examiner's rejection under § 112 is, therefore, respectfully requested.

* * * * *

It is noted that Applicants have voluntarily undertaken to amend the Specification for purposes of clarification, consistency and grammar, from the second full paragraph on page 29 through the first full paragraph on page 31. More particularly, the Specification is amended to clarify that the number of tokens N is a variable. In addition, since both M and N are variables, the use of both "M" and "N" is considered unnecessary. "N" is, therefore, substituted for "M" throughout the Specification. Applicants have also inserted appropriate "if-then" clauses, e.g., replacing "than" with - - then - -; changed "logged in" to - - logged on - - and "above-identified" to - - above-described - -; deleted "particular" from the phrase "this particular client", "its" from "its anticipation" and "that" from "each time that a first transmission", as redundant; added - - a - - before "large" in the phrase "anticipation of receiving large number of transactions"; and added - - of - - before "N" in the phrase "the value N". In this manner, Applicants respectfully submit that the invention has been better defined consistent with amendments made to related and co-pending U.S. Patent Application Serial No. 09/684,012, filed October 6, 2000, entitled "Method For Amortizing Authentication Overhead". Applicants respectfully state that no new matter has been added.

Regarding the Examiner Interview Summary dated September 14, 2004, Applicants, by their undersigned counsel, respectfully request correction of the Examiner's comments, as

follows: page 3, lines 2-3, of the Summary should read "Attorney relayed that the present invention is being sold at COMP USA as part of a remote monitoring system".

* * * * *

As for the rejection under § 103(a), Applicants respectfully disagree with the Examiner's reading and application of the cited references. First, Krishnamurthy et al. is directed to a network management system for operation over the Internet. Specifically, Krishnamurthy et al. teaches a Simple Network Management Protocol (SNMP) agent 82 and a Management Information Base (MIB) 72 that are adaptive in the sense that they adapt if the system is used with another protocol such as Common Management Information Protocol (CMIP). They do not adaptively determine the number of additional transmissions between a sender computer gateway/Web site and a receiver computer Web site/gateway, as set forth by Applicants, nor is there a number of additional transmissions variably and adaptively selected, at least in part, based upon the performance overhead of the system, monitored conditions, or set of criteria used in an algorithm to determine the number of additional transmissions.

Nickles relates to a network security system for providing a single point of access control to one or many source computers systems. Specifically, Nickles purports to enable a private network of computers associated with a particular entity, such as a bank, to be integrated with an open network while ensuring that transactions over the open network to the private network of computers is secure. Nickles specifically describes such computers as "devices or workstations" (e.g., column 7, lines 17-23), not Internet enabled devices, as claimed by Applicants.

As for Engel et al., this reference concerns a server and computer for manipulation and control of the way data packets are transmitted from an application to the network and how packets received from the network are passed to the application, including control of security (encryption and authentication) of one or more packets.

Contrary to Applicants' invention, as claimed, none of these references, whether taken alone or in any combination, disclose or suggest management of Internet enabled devices over the Internet, the step of adaptively determining the number of additional transmissions between a sender computer gateway/Web site and a receiver computer Web site/gateway, as set forth by Applicants, nor a number of additional transmissions variably and adaptively selected, at least in part, based upon the performance overhead of the system, monitored conditions, or set of criteria used in an algorithm to determine the number of additional transmissions. Applicants respectfully note, in this connection, that new claim 16 is added as directed to the "variably and adaptively selected" aspects set forth above.

* * * * *

Based on the foregoing, withdrawal of the Examiner's rejections under §§ 112, second paragraph, and 103(a) are respectfully requested.

Applicant has made a good faith attempt to place this Application in condition for allowance. Favorable action is requested. If there is any further point requiring attention prior to allowance, the Examiner is asked to contact Applicants' counsel at (212) 768-3800.

Please charge any additional fees that may be required to our firm Deposit Account No. 50-0518.

Respectfully submitted,

Dated: September 27, 2004

Grant E. Pollack, Esq.
Registration No. 34,097
Steinberg & Raskin, P.C.
1140 Avenue of the Americas, 15th Floor
New York, New York 10036
(212) 768-3800

Attorney for Applicants

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, in an envelope with sufficient postage addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

on September 27, 2004

Name Grant E. Pollack

Signature